

IN THE CLAIMS

1. (Currently Amended) A person identification certificate link system comprising an entity which forms a link correlating at least two certificates including a public key certificate which stores a public key serving as a cryptographic key and which is generated by a first certificate authority, and a person identification certificate which stores a template serving as person identification data and which is generated by a second certificate authority, thereby specifying one related certificate based on the other certificate;

wherein one of the public key certificate and the person identification certificate stores, as data, an identifier of a different certificate which is linked thereto, wherein said data includes a validity period for the respective certificates, and a group validity period is set to be equal to the shortest validity period of those of the certificates related to each other.

2. (Original) A person identification certificate link system according to Claim 1, wherein the link between the certificates comprises a link which relates the person identification certificate with the public key certificate of a public key applied to encrypt the template stored in the person identification certificate.

3. (Original) A person identification certificate link system according to Claim 1, wherein the link between the certificates comprises a link which relates the person identification certificate with the public key certificate which are both used to establish a connection with a data communication partner.

4. (Cancelled)

5. (Original) A person identification certificate link system according to Claim 1, wherein one of the public key certificate and the person identification certificate stores, as data, an identifier of a link structure serving as link identification data and identifiers of the linked public key certificate and person identification certificate.

6. (Original) A person identification certificate link system according to Claim 1, wherein group information including a group of identifiers of the linked public key certificate and person identification certificate is formed and managed as data separate from the certificates.

7. (Original) A person identification certificate link system according to Claim 1, wherein:

group information including a group of identifiers of the linked public key certificate and person identification certificate is formed and managed as data separate from the certificates; and
a link for specifying, based on the group information serving as primary information, secondary information related to the group information is formed.

8. (Original) A person identification certificate link system according to Claim 1, wherein one of the public key certificate and the person identification certificate stores a different certificate which is linked thereto.

9. (Previously Presented) A person identification certificate link system according to Claim 1, wherein the first certificate authority and the second certificate authority are formed as third-party agencies which are not users of the public key certificate and the person identification certificate.

10. (Currently Amended) An information processing apparatus for authenticating a person by comparing a template corresponding to person identification data acquired from sampling information input by a user, said information processing apparatus comprising an entity which encrypts and stores template information including the template; which obtains the encrypted template from a person identification certificate generated by a first certificate authority which is a third-party agency; which specifies a public key certificate generated by a second certificate authority which is a third-party agency in accordance with link information stored in the person identification certificate; which specifies a cryptographic key to the template based on the specified public key certificate; and which encrypts or decrypts the template;

wherein the person identification certificate stores, as data, an identifier of a different certificate which is linked thereto, wherein said data includes a validity period for the respective certificates, and a group validity period is set to be equal to the shortest validity period of those of the certificates related to each other.

11. (Currently Amended) An information processing apparatus for authenticating a person by comparing a template corresponding to person identification data acquired from sampling information input by a user, said information processing apparatus comprising an entity which obtains an encrypted template from a person identification certificate generated by a first certificate authority which is a third-party agency and which authenticates the person based on the template; and which specifies a public key certificate generated by a second certificate authority which is a third-party agency in accordance with link information stored in the person identification certificate and which performs mutual authentication or encrypted data communication with a data communication partner based on the specified public key certificate; wherein the person identification certificate stores, as data, an identifier of a different certificate which is linked thereto, wherein said data includes a validity period for the respective certificates, and a group validity period is set to be equal to the shortest validity period of those of the certificates related to each other.

12. (Currently Amended) An information processing method for authenticating a person by comparing a template corresponding to person identification data acquired from sampling information input by a user, said information processing method comprising the steps of:

encrypting and storing template information including the template;

obtaining the encrypted template from a person identification certificate generated by a first certificate authority which is a third-party agency;

specifying a public key certificate generated by a second certificate authority which is a third-party agency in accordance with link information stored in the person identification certificate, wherein the person identification certificate stores, as data, an identifier of a different certificate which is linked thereto, wherein said data includes a validity period for the respective

certificates, and a group validity period is set to be equal to the shortest validity period of those of the certificates related to each other;

specifying a cryptographic key to the template based on the specified public key certificate; and
encrypting or decrypting the template.

13. (Currently Amended) An information processing method for authenticating a person by comparing a template corresponding to person identification data acquired from sampling information input by a user, said information processing method comprising the steps of:

obtaining an encrypted template from a person identification certificate generated by a first certificate authority which is a third-party agency;

authenticating the person based on the template;

specifying a public key certificate generated by a second certificate authority which is a third-party agency in accordance with link information stored in the person identification certificate, wherein the person identification certificate stores, as data, an identifier of a different certificate which is linked thereto, wherein said data includes a validity period for the respective certificates, and a group validity period is set to be equal to the shortest validity period of those of the certificates related to each other;

and performing mutual authentication or encrypted data communication with a data communication partner based on the specified public key certificate.

14. (Currently Amended) A program providing medium for providing a computer program that causes a computer system to authenticate a person by comparing a template corresponding to person identification data acquired from sampling information input by a user, said computer program performing the steps of:

encrypting and storing template information including the template; and

obtaining the encrypted template from a person identification certificate generated by a first certificate authority which is a third-party agency;

specifying a public key certificate generated by a second certificate authority which is a third-party agency in accordance with link information stored in the person identification certificate, wherein the person identification certificate stores, as data, an identifier of a different certificate which is linked thereto, wherein said data includes a validity period for the respective certificates, and a group validity period is set to be equal to the shortest validity period of those of the certificates related to each other;

specifying a cryptographic key to the template based on the specified public key certificate; and

encrypting or decrypting the template.

15. (Currently Amended) A program providing medium for providing a computer program that causes a computer system to authenticate a person by comparing a template corresponding to person identification data acquired from sampling information input by a user, said computer program performing the steps of:

obtaining an encrypted template from a person identification certificate generated by a first certificate authority which is a third-party agency;

authenticating the person based on the template;

specifying a public key certificate generated by a second certificate authority which is a third-party agency in accordance with link information stored in the person identification certificate, wherein the person identification certificate stores, as data, an identifier of a different certificate which is linked thereto, wherein said data includes a validity period for the respective certificates, and a group validity period is set to be equal to the shortest validity period of those of the certificates related to each other; and

performing mutual authentication or encrypted data communication with a data communication partner based on the specified public key certificate.